STATEMENT OF RICHARD L. SKINNER

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON MANAGEMENT, INTEGRATION, AND OVERSIGHT

COMMITTEE ON HOMELAND SECURITY

U.S. HOUSE OF REPRESENTATIVES

APRIL 20, 2005

Good morning Mr. Chairman and Members of the Committee:

I am Richard L. Skinner, Acting Inspector General for the Department of Homeland Security (DHS). Thank you for the opportunity to be here today to discuss the work of the Office of Inspector General (OIG) regarding major management challenges facing DHS.

During its first two years of existence, DHS worked to accomplish the largest reorganization of the federal government in more than half a century. Creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack, presented an inordinate number of challenges to the department's managers and employees. The Government Accountability Office (GAO) noted that successful transformations of large organizations, under even less complicated situations, could take from five to seven years. While DHS has made great strides toward improving homeland security, it still has much to do to establish a cohesive, efficient, and effective organization.

Based on our work, as well as assessments by Congress, GAO, and DHS itself, the OIG identified "major management challenges" facing the department. These challenges, included in the department's Performance and Accountability Report issued on November 15, 2004, are a major factor in setting our priorities for audits and inspections of DHS programs and operations. As required by the *Reports Consolidation Act of 2000*, we update our assessment of management challenges annually.

Our latest major management challenges report covers a broad range of issues, including both program and administrative challenges. A copy of that report is provided for the record. In its response to the report, the department recognized the challenges and the potential impact the challenges could have on the effectiveness and efficiency of its programs and operations if not properly addressed. The department anticipates that the results of initiatives to address the challenges during FY 2005 should enable it to report significant progress next year.

Before I discuss the challenges and the details of our work, I believe it is important that we give credit to the thousands of dedicated, hard working DHS employees who are genuinely committed to securing our homeland and making the department a model for the entire federal government. No one here can deny that our nation is more secure today than it was prior to September 11, 2001.

I also wish to point out that the department has been responsive to and implemented a number of the recommendations made by our office. We look forward to establishing
a positive working relationship with the new Secretary, and continuing the momentum toward building an effective, efficient, and economical homeland security operation -- one that is free of fraud, waste, and abuse.

BORDER SECURITY

A primary mission of DHS is to reduce America's vulnerability to terrorism by protecting the borders of the U.S. and safeguarding its transportation infrastructure. Within DHS, these responsibilities fall to the Border and Transportation Security (BTS) Directorate.

Two organizations within BTS are responsible for enforcing the nation's immigration and customs laws. Customs and Border Protection (CBP) inspects visitors and cargoes at the designated U.S. ports of entry (POE), and secures the borders between the POE. CBP's primary mission is to prevent terrorists and terrorist weapons from entering the U.S., while also facilitating the flow of legitimate trade and travel. Immigration and Customs Enforcement (ICE) is the investigative arm of BTS that enforces immigration and customs laws within the U.S. While CBP's responsibilities focus on activities at POEs and along the borders, ICE's responsibilities center on enforcement activities related to criminal and administrative violations of the immigration and customs laws of the U.S., regardless of where the violation occurs. Additionally, CBP and ICE have employees assigned outside the U.S. to enhance the security of our borders.

In December 2004, the Heritage Foundation recommended merging CBP and ICE and eliminating the Border and Transportation Security directorate. According to the Foundation, the merger would bring together all of the tools of effective border and immigration enforcement – inspectors, border patrol agents, special agents, detection and removal officers, and intelligence analysts – and realize the objective of creating a single border and immigration enforcement agency. Eliminating BTS would remove a middle management layer allowing the combined CBP-ICE to report directly to the Secretary via the Deputy Secretary. On January 26, 2005, Chairman Collins asked our office to study this proposal and to report our conclusions and recommendations in 180 days. We are in the midst of our field work now and expect to meet this deadline.

The third organization within BTS which plays a major role in protecting the borders of the U.S. and safeguarding its transportation infrastructure is the Transportation Security Administration (TSA). TSA's primary security improvements have focused on aviation, with the hiring of over 60,000 passenger and baggage screeners, installation of electronic passenger and baggage screening technology at the nation's airports, and expansion of the Federal Air Marshals program, which is located now in ICE.

Other organizations within BTS have border security related responsibilities as well, such as the US-VISIT Program Office and the Federal Law Enforcement Training Center (FLETC). The US-VISIT Program Office is responsible for the development and fielding of the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, DHS' entry-exit system. It coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). FLETC, another BTS component, provides career-long law enforcement training to 81 federal partner organizations and numerous state, local, and international law enforcement agencies.

And, the U.S. Citizenship and Immigration Services (USCIS), although not organizationally housed within BTS, plays an important part in DHS border security. USCIS is responsible for reviewing and approving applications for immigration benefits. While not a law enforcement agency, USCIS ensures that only eligible aliens receive immigration benefits and identifies cases of immigration benefit fraud and other immigration violations that warrant investigation.

As expected, DHS faces several formidable challenges in securing the nation's borders. Our audit and inspection program has attempted to address some of the challenges, including: developing effective visa issuance programs; tracking the entry and exit of foreign visitors; and, preventing terrorist weapons from entering the United States.

Visa Issuance Programs

As the Heritage Foundation's report aptly pointed out, our nation's homeland security does not stop at America's geographic borders. DHS faces international challenges in protecting our borders, too. Provisions in the visa issuance process and other programs to promote international travel create potential security vulnerabilities, which may allow terrorists, criminals, and other undesirables to enter the U.S. undetected.

For example, DHS must address security concerns identified in the Visa Waiver Program (VWP). The VWP enables citizens of 27 countries to travel to the U.S. for tourism or business for 90 days or less without obtaining a visa. These travelers are inspected at a U.S. POE, but they have not undergone the more rigorous background investigations associated with visa applications. In an April 2004 inspection, we reported our concerns regarding the exclusion from the US-VISIT program of travelers under the VWP. In September 2004, BTS began requiring that travelers from VWP countries enroll in the US-VISIT program, and renewed its efforts to conduct required country reviews.

However, DHS continues to experience problems in identifying and detecting aliens who present lost or stolen passports from VWP countries at ports of entry. Shortcomings in procedural and supervisory oversight permitted some aliens presenting stolen Visa Waiver Program passports to enter the United States even after their stolen passports were reported, watch-listed, and detected. New information on lost and stolen passports provided by Visa Waiver Program governments was not routinely checked against U.S. entry and exit information to determine whether the stolen passports have been used to enter the U.S. In addition, there was no formal protocol for providing information concerning the use of stolen passports to ICE for investigation and apprehension of the bearer.

Problems with lost and stolen passport are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify *mala fide* travelers using stolen Visa Waiver Program passports - even when the theft has been reported and the information is available in DHS lookout systems. This occurs because stolen passports are reported using the passports' inventory control numbers (ICNs), which are entered into the lookout systems. However, when inspectors routinely enter just the passports' issuance numbers into the lookout systems and do not match the reported stolen ICNs, the result is undetected stolen passports. While we applaud BTS' efforts to promote a change in the International

Commercial Aviation Organization standard to a one-number passport system, it will take years once the new standard is adopted for the two-number passports to be removed from service. Interim measures are needed to reduce this vulnerability. In response to these concerns, BTS is conducting systematic reviews of admission records to check for previous uses of newly-stolen passports.

Further, DHS must address issues identified with its visa security program, under which DHS stations officers at U.S. embassies and consular offices overseas to review visa applications and perform other law enforcement functions. Because of limited resources, BTS used temporary duty officers in its pilot effort who often did not have the required background or training, including language skills, to perform effectively as visa security officers. For example, nine of the ten temporary duty officers who served or are serving in Saudi Arabia did not read or speak Arabic. This limits their effectiveness and reduces their contribution to the security of the visa process. In response to our report, BTS advised that it would stop using temporary duty officers and begin using permanently assigned officers at its visa security offices; develop a staffing model to ensure only qualified officers serve in these positions; and, develop a training program for visa security officers. While BTS agreed with us in principle regarding the need for language training, BTS officials said that because of funding concerns, it could provide language training only "as necessary and to the extent possible."

As a result, the full intelligence and law enforcement value that visa security officers could add to the existing inter-agency country teams has not been achieved. In response to our report, DHS advised that it has developed a near-term plan for deploying visa security officers for FY 2005 and was planning for additional deployments.

With respect to international travelers, two major border security challenges confront the department: the divergence in the biometric systems used to identify travelers; and, the substantial differences in the levels of scrutiny given to different classes of travelers.

Biometric Systems

We have all seen the glaring deficiencies of name-based lookout lists. For every known terrorist there are many innocent people with the same name. And for every name, there are variants and misspellings. Biometric identifiers are the only reliable and practical way to tell people apart.

The FBI uses ten rolled fingerprints in the IAFIS to document criminal activities. The former INS, now within DHS, used only two index finger prints to create retrievable records for travelers in its Automated Biometric Identification System (IDENT). As reported, the two systems have not yet been integrated, so some travelers are run through one system - and then sometimes the other - at ports of entry. The CBP agents are required to check both systems when illegal aliens are apprehended.

The international standards for passports are developed through ICAO. The United States is one of several countries whose citizens are not fingerprinted routinely for licenses or identification cards. In the past, the U.S. has lobbied ICAO to use facial recognition rather than fingerprints as the required primary biometric identifier in passports. Public accounts suggest that the

experiments to date using facial recognition (at Logan Airport, among others) yielded meager results. At our borders, meanwhile, we increasingly rely upon fingerprint scans to tell people apart. The difficulties in achieving international consensus on this subject are daunting. Far more obvious, however, is the fact that the United States cannot afford to implement both biometric capabilities at each port of entry, it must settle on one. We – the United States Government – need to decide soon which biometric is the most reliable. Then we need to apply that standard to our own identity and travel documents, as well as for foreign travelers. We cannot do this in a vacuum, however. We need international cooperation to establish a global standard.

Levels of Scrutiny

The second challenge relates to the inconsistent levels of scrutiny to which travelers are subjected. Everyone knows that some non-immigrants need visas, but others do not. Less well known is that some do not even require passports. Immigrants, some of whom spend little time in the U.S., receive medical examinations and background checks, but non-immigrants, some of whom remain here legally for many years, do not.

Usually, travelers from visa waiver countries do not require visas but, depending on the claimed purpose of their trip, they sometimes do. Most citizens of Canada and Mexico do not need visas or passports to enter the United States. We do not always record their names, or check them against our databases, though we do check their automobile license plates at land POEs. During FY 2002, 104 million visa-exempt Mexicans constituted 24 percent, and 52 million visa-exempt Canadians constituted 12 percent, of all admissions.

U.S. citizens reenter the country with the least scrutiny of all, and frequently require no passport. Foreign travelers who can successfully pretend to be Americans get the same special treatment, as documented by the GAO in its May 2003 report, "Counterfeit Documents Used to Enter The United States From Certain Western Hemisphere Countries Not Detected" (03-713T).

The US-VISIT system screens only non-immigrants with visas, or visitors using the provisions of the Visa Waiver Program. According to fiscal year 2002 statistics, the approximately 15 million VWP visitors accounted for three percent of U.S. admissions, while 19 million travelers with nonimmigrant visas accounted for five percent. In essence, US-VISIT screens fewer than nine percent of the people entering the United States. In our review of the implementation of US-VISIT at land POEs, issued in February 2005, we noted that at land borders, where travelers with visas or using the VWP are a rarity, the percentage of crossers screened by US-VISIT is very small: less than three percent.

No one designing a border security system from the ground up would create such a hodge-podge of processes with so many potential security gaps. If we are to be serious about border security, we will need to rationalize our border crossing processes. People are not always who they claim to be, and terrorists and criminals will try to assume whichever false identity will get them the least scrutiny as they enter and depart our country.

Tracking the Entry and Exit of Foreign Visitors

Keeping track of people entering and leaving the U.S. is necessary to prevent terrorism, narcotics smuggling, and illegal alien smuggling, as well as to enforce trade laws and collect revenue, all while facilitating international travel. Over the next five years, DHS will invest billions of dollars to modernize the passenger processes and systems inherited from the legacy agencies, including the US-VISIT system. Concerted efforts are now being made to realign certain operations and systems within the newly created DHS.

However, DHS did not analyze or re-examine its strategy, processes, technology, and organization for the overall federal passenger processing requirements before proceeding with US-VISIT. Further, DHS did not have an overall modernization acquisition strategy for the legacy Customs, INS, TSA, or the Animal and Plant Health Inspection Service (APHIS) systems related to passenger processing. An acquisition strategy based on a re-engineered vision of how DHS will process international travelers, in alignment with the department's enterprise architecture, should result in better and more definitive contract requirements.

We recommended that BTS initiate a business process reengineering effort to establish a clear vision of the overall federal operations that will be used to clear people entering and leaving the U.S. Based on those results, BTS should work with the Chief Acquisition Officer (CAO) and Chief Information Officer (CIO) to develop an overall departmental acquisition strategy for passenger information technology systems. BTS advised that it plans to initiate a business process reengineering effort, and develop an overall department acquisition strategy in coordination with the CAO and CIO.

Finally, in a report issued in June 2004, we raised concerns about the Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program. This program permits pre-screened and enrolled low risk travelers to enter the U.S. from Mexico in designated lanes with minimal inspection by CBP officers, thereby avoiding the lengthy waiting times in the regular inspection lanes. The SENTRI program is open to both U.S. citizens and certain non-citizens. We determined that the program is generally achieving the two basic objectives for which it was established: accelerating the passage of participating travelers through land ports of entry; and, maintaining border integrity, security, and law enforcement responsibilities.

However, we noted inconsistencies in the way land ports of entry applied eligibility criteria for criminal offenses, financial solvency, and residency, and approved or denied applications. In addition, we noted weaknesses in the procedures by which SENTRI system records are kept current, and how alerts are disseminated to CBP officers. Taken as a whole, our findings indicate weak program management that could jeopardize the program's integrity and border security. In response to these concerns, CBP has moved to merge all of its trusted travelers programs and centralize the enrollment process to standardize enrollment procedures and criteria.

Preventing Terrorist Weapons from Entering the U.S.

Since September 11, 2001, CBP's priority mission is detecting and preventing terrorists and terrorist weapons from entering the U.S. A major component of its priority mission is to ensure that oceangoing cargo containers arriving at seaports of entry are not used to smuggle illegal or dangerous contraband. To test controls over importing weapons of mass destruction, ABC News

was successful twice at smuggling depleted uranium into the country. On September 11, 2002, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium was shipped from Europe to the U.S. undetected by CBP. On September 11, 2003, ABC News reported that the same cylinder was smuggled - again undetected - to the U.S. from Jakarta, Indonesia.

In the first smuggling event, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium, which was shielded with lead, was placed in a suitcase and accompanied by reporters by rail from Austria to Turkey. In Istanbul, Turkey, the suitcase was placed inside an ornamental chest, which was crated and nailed shut. The crate containing the suitcase was placed alongside crates of huge vases and Turkish horse carts in a large metal shipping container, and then loaded onto a ship, which left Istanbul. Based on data contained in the Automated Targeting System, the crate was targeted as high-risk for screening by the U.S. Customs Service. ABC News broadcast on September 11, 2002, that Customs failed to detect the depleted uranium carried from Europe to the United States.

During the second smuggling event, ABC News placed the same cylinder of depleted uranium into a suitcase, and then placed the suitcase into a teak trunk. The trunk, along with other furniture, was loaded into a container in Jakarta, Indonesia, and then transshipped to the U.S. from Tanjung Pelepas, Malaysia. This shipment, which was targeted as high-risk for screening and subsequently inspected by CBP personnel, was then allowed to proceed from the port by truck.

In a classified September 2004 report, we cited several weaknesses that occurred at the time of the two incidents, which made the container inspection process ineffective. The protocols and procedures that CBP personnel followed at the time of the two smuggling incidents were not adequate to detect the depleted uranium. CBP has since enhanced its ability to screen targeted containers for radioactive emissions by deploying more sensitive technology at its seaports, revising protocols and procedures, and improving training of CBP personnel.

We are currently conducting a follow-up audit on the issue of radiation detection. The audit will determine to what extent CBP has a complete and workable plan for deploying and effectively operating radiation portal monitors at major U.S. seaports, and how the new technologies that CBP is deploying will impact operations at the ports.

TRANSPORTATION SECURITY

DHS faces significant challenges in ensuring the security of the nation's transportation systems. TSA and the Coast Guard spearhead the department's transportation security efforts. While TSA has made progress in implementing the *Aviation and Transportation Security Act* (ATSA) and securing the nation's airways, improvements are still needed in aviation, rail, and transit security. Similarly, the Coast Guard has made progress in securing the nation's maritime transportation system but the deteriorating condition of its aircraft and cutter fleets places its current and future mission performance at risk.

Aviation Security

The success of TSA in fulfilling its aviation security mission depends heavily on the quality of its staff and the capability and reliability of the equipment to screen passengers and cargo to identify terrorists and terrorists' weapons, while minimizing disruption to public mobility and commerce.

Providing qualified and trained personnel has been a substantial challenge for TSA. ATSA mandated that the TSA hire and train thousands of screeners for the nation's 429 commercial airports by November 19, 2002. As a result, TSA hired over 60,000 screeners. Our undercover tests of screener performance, about which we first reported in 2004, revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not carried into the sterile areas of heavily used airports, or do not enter the checked baggage system. We attributed the test failures to four areas that needed improvement: training; equipment and technology; policy and procedures; and, management and supervision. TSA agreed with our recommendations and took action to implement them, particularly in the areas of training, policies and procedures, and management practices. We recently completed a follow-up review of screener performance at the same airports. We began our review at the end of November 2004 and completed our fieldwork in early February 2005. Despite the fact that the majority of screeners with whom our testers came in contact were diligent in the performance of their duties and conscious of the responsibility those duties carry, the lack of improvement since our last audit indicates that significant improvement in performance may not be possible without greater use of new technology.

We recommended in our previous report that the TSA administrator aggressively pursue the development and deployment of innovations and improvements to aviation security technologies, particularly for checkpoint screening. TSA is currently testing several such technologies, including backscatter x-ray, Explosive Trace Detection (ETD) portals, and document scanners. We encourage TSA to expedite its testing programs and give priority to technologies, such as backscatter x-ray, that will enable the screening workforce to better detect both weapons and explosives.

Furthermore, TSA has come under criticism for not moving quickly enough to address the vulnerability of the nation's air traffic to suicide bombers. The 9-11 Commission recommended that TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As noted above, TSA is in the process of testing several of these technologies, including backscatter x-ray, vapor detection, and document scanner machines, to address concerns regarding detection of explosives on individuals. Pending the testing and deployment of these advanced technologies, TSA instituted a process of more extensive pat-down procedures to find explosives hidden on a traveler. Since travelers and interest groups protested the use of these more thorough examination procedures, they have already been refined by TSA. We are currently reviewing the implementation of these procedures to ensure they are strictly followed, as well as TSA's process for responding to passenger complaints.

Rail and Transit Security

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across other modes of transportation. More than 6,000 agencies provide transit services through buses, subways, ferries, and light-rail to about 14 million Americans. Terrorist experiences in Madrid and Tokyo highlight potential vulnerabilities in transit systems. Recently, several congressional leaders expressed concern that the federal government has not responded strongly enough to the threat to public transit. Furthermore, the 9/11 Commission reported that over 90% of the nation's $5.3 billion annual investment in TSA goes to aviation, and that current efforts do not reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits so that transportation security resources can be allocated where the risks are greatest in a cost effective way. TSA's FY 2005 budget still focuses its resources on aviation.

TSA has lead responsibility for coordinating the development of a transportation sector plan, which it plans to complete later this year. TSA, however, has not finalized the memoranda of understanding with various Department of Transportation agencies to determine how it will coordinate work in the future. We are evaluating TSA's actions to assess and address potential terrorist threats to the mass transit systems of U.S. metropolitan areas.

Maritime Security

The Coast Guard's willingness to work hard and long hours, use innovative tactics, and work through partnerships in close inter-agency cooperation has allowed it to achieve mission performance results. However, to improve and sustain its mission performance in the future, the Coast Guard faces a significant barrier in overcoming the deteriorating

readiness of its fleet assets. The Coast Guard faces three major barriers to improving and sustaining its readiness to perform legacy missions:

1. The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance.

2. The workload demands on the Coast Guard will continue to increase as it implements the *Maritime Transportation Security Act of 2002* (MTSA). This complex work requires experienced and trained personnel; however, the Coast Guard has suffered from declining experience levels among its personnel in recent years.

3. Sustaining a high operating tempo due to growing homeland security demands - such as added port, waterway, and coastal security patrols - will tax the Coast Guard's infrastructure, particularly its aging cutter and aircraft fleet.

The lack of a comprehensive and fully defined performance management system impeded the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to define a performance management system that includes all the input, output, and outcomes needed to gauge results or target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crises or major terrorist attacks. For example, for search and rescue, the number of mariners in distress saved is a good indicator of outcome. However, resource hours under-represent the effort put into this mission by omitting the many hours of watch standing at stations. Without more complete information, the Coast Guard has limited ability to identify and target cost effective improvements to its mission performance.

The workload demands on the Coast Guard will continue to increase as it implements the MTSA. Under MTSA, the Coast Guard must conduct risk assessments of all vessels and facilities on or near the water; develop national and area maritime transportation security plans; and, approve port, facility, and vessel security plans. This complex work requires experienced and trained personnel, presenting a major challenge for the Coast Guard, which suffers from declining experience levels among its personnel. Since the Coast Guard largely relies on experienced senior personnel to coach and train junior personnel and new recruits on the job, mission performance is at risk.

In addition to implementing MTSA, growing homeland security demands the agency, such as added port, waterway, and coastal security patrols, result in a continued high operating tempo. Sustaining this high operating tempo will be a major challenge for Coast Guard personnel and will tax its infrastructure, especially its aged cutter and aircraft fleet. The Coast Guard reported that sustaining its mission is at risk due to cutters and aircraft which are aging, technologically obsolete, or those which require replacement and modernization. Currently, the Coast Guard is experiencing serious cracking in the hulls of the 110-foot cutters and engine power loss on the HH-65 Dolphin helicopters, resulting in operating restrictions. These problems adversely affect the Coast Guard's mission readiness and ultimately mission performance.

Maintaining and Replacing Deepwater Assets.

In June 2002, the Coast Guard awarded a $17 billion contract to Integrated Coast Guard Systems to maintain and replace its Deepwater assets. This contract called for replacing or modernizing, by 2022, all assets used in missions that occur more than 50 miles offshore, including approximately 90 cutters and 200 aircraft as well as assorted sensors and communications systems. According to the Coast Guard, the greatest threat to its missions continues to be the operational capability of its legacy aircraft, cutter, and small boat fleet. These assets are aging and are more expensive to maintain. In some instances, the Coast Guard is experiencing difficulty maintaining and upgrading existing critical deepwater legacy assets including the HH-65, HH-60, HC-130 aircraft, and its coastal patrol boat fleets.

As an example, the number of in-flight loss of power mishaps involving the HH-65 helicopter grew from about a dozen annual mishaps before September 11, 2001, to more than 150 in FY 2004, requiring the immediate re-engining of the entire HH-65 fleet. The Coast Guard recently accelerated its acquisition of the Multi-Mission Cutter Helicopter under development by the Integrated Deepwater System acquisition project, in addition to initiating engine replacement for its HH-65 helicopter fleet. Also, in 2003, the Coast Guard experienced 676 unscheduled maintenance days for its cutters—a 41% increase over 2002. This was the equivalent of losing the services of over three and a half cutters. These lost cutter days include the coastal patrol boats, which are suffering from accelerated hull corrosion and breached hull casualties.

INTEGRATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components into a single, effective, efficient, and economical department remains one of DHS' biggest challenges. To help meet this challenge, DHS established an Operational Integration Staff to assist departmental leadership with the integration of certain DHS missions, operational activities, and programs at the headquarters level and throughout the regional structure.

Much remains to be done in integrating DHS programs and functions. We have reported that structural and resource problems continue to inhibit progress in certain support functions. For example, while the department is trying to integrate and streamline support service functions, most of the critical support personnel are distributed throughout the components and are not directly accountable to the functional Line of Business (LOB) Chiefs such as the Chief Financial Officer, Chief Information Officer, Chief Human Capital Officer, Chief of Administrative Services, and Chief Procurement Officer.

In August 2004, the Secretary and Deputy Secretary directed the DHS LOB chiefs to design and implement systems to optimize functions across the entire department. The LOB chiefs were instructed to develop Management Directives to guide the department's management of those business functions, too. The Directives were to be built on a concept of "dual accountability," where both the operational leadership and the LOB chiefs are responsible for the successful preparation of the Directives and their implementation. This concept has been described as a "robust dotted line" relationship of agency or component functional heads to the LOB chiefs for both daily work and annual evaluation. In October 2004, the Secretary signed Final Management

Directives to institutionalize the arrangements before FY 2005. In addition, the department's Management Council signed charters for each LOB, which establish a formal governance and advisory board structure to ensure that the objectives and intent of the Directives are executed.

While the concept underlying the Management Directives may work in some environments, we are concerned that the DHS LOB chiefs may not have sufficient resources or authority to ensure that department-wide goals and challenges in their respective functions are addressed effectively, efficiently, or economically - or that available resources can be marshaled to address emerging problems. These concerns were heightened by the department's experience this past fiscal year in reorganizing the former Immigration and Naturalization Service (INS) and the U.S. Customs Service into three new bureaus – Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS) - referred to as the "tri-bureaus" – and the consolidation of accounting services for many small programs outside of DHS into ICE. Since the department and ICE did not prepare a thorough, well-designed plan to guide the transition of accounting responsibilities, ICE fell seriously behind in the performance of basic accounting functions, such as account reconciliations and analysis of abnormal balances. The pervasiveness of errors in ICE's accounts prevented completion of audit work at ICE for the FY 2004 DHS financial statement.

Additionally, the department faces a structural problem in its financial management organization. The bureaus control most of DHS' accounting resources, but the DHS Chief Financial Officer (CFO) has responsibility for DHS' consolidated financial reporting, which is dependent on those resources. Although coordination mechanisms are in place, the monitoring controls at the DHS CFO's level are insufficient to ensure the accuracy of consolidated financial information. The seriousness of these material weaknesses and reportable conditions at DHS demands strong oversight and controls.

Similarly, creating a single infrastructure for effective communications and information exchange remains a major management challenge for DHS. We reported in July 2004, that the DHS CIO is not well positioned to meet the department's IT objectives. The CIO is not a member of the senior management team with authority to strategically manage department-wide technology assets and programs. No formal reporting relationship is in place between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for central IT direction. Further, the CIO has limited staff resources to carry out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-making, and a reliance instead on cooperation and coordination within DHS' CIO Council to accomplish department-wide IT integration and consolidation objectives[1]. The department would benefit from following the successful examples of other federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on department-wide IT investments and strategies.

In this regard, the Secretary is reexamining selected operations in what he refers to as a "second stage review." The review will cover where DHS has been, where it's headed, and what changes, if any, need to be made.

We will be monitoring and evaluating the progress made in each LOB area very closely, not only during FY 2005, but also for years to come.

INFORMATION SECURITY

The DHS Chief Information Officer (CIO) oversees the information security program. The CIO has developed an Information Security Program Strategic Plan to provide the foundation for an agency-wide, consolidated information security program. The DHS Chief Information Security Officer (CISO) developed the Information Security Program Management Plan, which is the blueprint for managing DHS' information security program. At the same time, the CISO developed an Information Security Risk Management Plan, which documents DHS' plan to develop, implement, and institutionalize a risk management process in support of its information security program. Based on our review of these plans, DHS has an adequate structure, blueprint, and process to implement and manage its information security program.

Our office performs a yearly review of the DHS information security program as required by the *Federal Information Security Management Act of 2002* (FISMA). During our FY 2004 review, we noted that DHS made significant progress over the last two years to develop, manage, and implement its information security program. However, DHS' organizational components have not fully aligned their respective security programs with DHS' overall policies, procedures, or practices. Factors which have kept the department from having an effective information security program include: lack of a system inventory; lack of a formal reporting structure between the CIO and the organizational components; lack of a verification process to ensure that all information security weaknesses have been identified; and, all of the department's major information systems have not been certified and accredited.

Overall, DHS is on the right track to create and maintain an effective information security program. However, the department and its components still have much work to do to get to the point where DHS has a mature information security program.

INTELLIGENCE

Under the *Homeland Security Act of 2002*,[1] the department is responsible for receiving, integrating, and coordinating the sharing of federal information to help ensure border security and protect the U.S. from terrorist threats. Specifically, the *Homeland Security Act of 2002* gave DHS significant responsibility to coordinate the sharing of information to protect the U.S. from terrorist threats. The law requires that the DHS Under Secretary for Information Analysis and Infrastructure Protection (IAIP) consult with the Director of Central Intelligence and other appropriate intelligence and law enforcement elements of the federal government to establish collection priority and strategy for information relating to threats of terrorism against the U.S.[2] Additionally, the law directs the IAIP Under Secretary to review, analyze, and make recommendations to improve the policies and procedures governing the sharing of law enforcement, intelligence, intelligence-related, and other information relating to homeland security.[3].

However, the role and responsibilities of IAIP for intelligence collection, analysis, and dissemination has been abated with the creation of the Terrorist Threat Integration Center under the Director of Central Intelligence and the Terrorist Screening Center under the Director of the FBI. Creation of the new Director of National Intelligence position makes the DHS intelligence coordination role even more uncertain, calling for prompt clarification of federal lines of authority in this area.

PREPAREDNESS

To date, our office focused on examining the programs and mechanisms that enhance preparedness at the federal, state, and local levels of government, including the utility of IAIP data on port security grant award decisions. In its December 2004 report, the Heritage Foundation recommended consolidating DHS critical infrastructure protection and preparedness, as well as state, local, and private coordination efforts, under an Undersecretary for Protection and Preparedness. According to the Foundation, consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state, local, and private sector entities on securing those vulnerabilities and preparing for attacks, and make grants to help get the job done and to induce cooperation. Again, on the surface, this proposal appears to have merit. However, since we have not studied the implications of this proposal, we are not in a position to address the pros and cons of such a consolidation. Nevertheless, we do have reservations about separating FEMA's preparedness functions from its response and recovery responsibilities. Disaster preparedness, response, and recovery are intricately related, each relying on the other for success. This proposal should be carefully studied before it is put into practice.

Also, the Department just completed TOPOFF3, said to be one of the largest incident response exercises in the world, involving three nations and over 10,000 participants. Our office

[1] Public Law 107-296 (Nov. 25, 2002), codified at 6 USC 101 *et seq*.
[2] 6 USC 121 (d)(10).
[3] 6 USC 121 (d)(8).

monitored the exercise here and at two venues in New Jersey and Connecticut. The after-action reports are not final. It is important that we learn from these exercises and put the lessons to work in new preparedness strategies and exercises as quickly and aggressively as possible.

Infrastructure Protection

One of the significant challenges facing the new DHS Secretary is the need to base the department's business decisions, such as its grant awards, on information relating to nationally critical infrastructure and key assets. We learned from two surveys completed in 2004 and a more recent review of DHS' Port Security Grant program issued in January 2005, that the department lags in integrating critical asset data and its "preparedness" initiatives into its business decisions. We concluded in 2004, too, that if IAIP did not produce a condensed list of most sensitive critical assets other elements within DHS would be at risk of failing to direct their grant resources toward national critical infrastructure protection and preparedness. This concern materialized in port security grant awards: administrators designed and operated the program as a sector-specific grant program and conducted at least three rounds of grants, totaling $560 million, without definitive national priorities for securing the seaport infrastructure of the nation. Poor integration of critical asset information meant that port security grant award decisions were made without sufficient information about our national priorities. DHS components need to strengthen their working relationships with IAIP, which has primary responsibility within DHS for critical asset identification, prioritization, and protection. The department's investments in new technologies, systems, and grant-making programs must reflect national priorities as determined by IAIP's risk management activities.

A lack of coordination between the Science and Technology Directorate (S&T) and other DHS components slowed S&T's long-term plan to invest in threat vulnerability and risk assessment tools, too. S&T is required to coordinate with other executive agencies, particularly those within DHS, to: (1) develop an integrated national policy and strategic plan for identifying and procuring new technologies; (2) reduce duplication and identify unmet needs; and, (3) support IAIP in assessing and testing homeland security vulnerabilities and possible threats. TSA, the Coast Guard, and IAIP have developed risk assessment tools and performed analyses of critical infrastructure. It is critical for the S&T to have a clear understanding of the terrorist threat picture facing the nation and the current technical capabilities and ongoing research and development initiatives of other DHS elements. To be effective, it must be able to prioritize its investment decisions, and avoid duplicating technology initiatives by other DHS components, especially in the area of risk assessment. To that end, the extent that the Secretary oversees these efforts and makes intra-agency coordination a reality, will determine his effectiveness in ensuring that DHS' investments are adequately matched to risk.

We are seeing signs that IAIP is becoming more involved in risk assessment activity and grant decision-making across the department as agencies are increasingly seeking assistance from IAIP. S&T has intensified efforts to obtain terrorist threat information from IAIP and incorporate it into S&T's selection of new technologies. The Coast Guard is working closer with IAIP on maritime risk assessments and programs. Grant officials signaled their intention to consult IAIP and make better use of critical infrastructure information in future rounds of port security grants.

The Secretary needs to ensure that this progress continues and becomes a regular part of DHS's business decision-making. DHS components must share information, assimilate data to better coordinate risk management activities, and subscribe to a single concept of national priorities and interests. These actions are the foundation of solid business judgments now and in the future. Without this leadership, DHS risks having multiple, confusing, and possibly conflicting sources of priority for its investments.

CONTRACT MANAGEMENT

DHS obligated about $13 billion to procure goods and services during FY 2003 and 2004. In addition to the challenge of integrating the procurement functions of its component organizations, DHS must provide contract management to the departmental components, which came into the agency without accompanying procurement staff. These components include the Science & Technology Directorate, the Information Analysis & Infrastructure Protection Directorate, the Office of State and Local Government Coordination and Preparedness, U.S. VISIT, and other offices.

DHS formed the Office of Procurement Operations (OPO) to provide procurement support for these components. But, the office has insufficient staff to manage over $2.5 billion in procurements. Therefore, DHS contracted with other federal agencies to provide the contract management support needed while it addresses the resource issues in OPO. However, providing consistent contract management throughout DHS remains a formidable challenge. The OPO developed and negotiated with its customer organizations a staffing plan that would bring OPO's staffing level to 127 by the end of FY 2005. The cost of these positions would be reimbursed by customer organizations through the Working Capital Fund.

DHS' efforts to provide a sufficiently detailed and accurate listing of its procurement information proved difficult. While DHS has migrated all of its procurements under the umbrella of one comprehensive reporting system, the department still lacks sufficiently detailed and validated data to manage the procurement universe and ensure accurate or consistent reporting.

While the DHS organizational components face continuing challenges in contract management, they have made some progress. For example, the Transportation Security Administration (TSA) relies extensively on contractors to accomplish its mission, although it provided little contract oversight during its first year of operation. As a result, the cost of some of those initial contracts ballooned. For example, TSA improperly administered one of these contracts as cost-plus-percent-of-cost and paid at least $49 million in excessive profit to the contractor. In 2004, however, TSA began implementing policies and procedures to provide adequate procurement planning, contract structure, and contract oversight.

Several other components of the department have large, complex, high-cost procurement programs under way that need to be closely managed, too. For example, CBP's Automated Commercial Environment project will cost $5 billion, and the Coast Guard's Deepwater Capability Replacement Project will cost $17 billion and take two-three decades to complete. Further, the department recently awarded a $10 billion contract for the development of a system to support the United States Visitor and Immigrant Status Indication Technology (US-VISIT)

program to track and control the entry and exit of all aliens through U.S. air, land, and sea ports of entry. It is anticipated that this program will be implemented over the next ten years. Also, TSA's managed information technology services contract will cost over $1 billion.

We will continue to review these major procurements. Recently, Secretary Chertoff expressed concerns regarding the vulnerability of DHS procurements to fraud, waste, and abuse. At his request, the OIG and Office of the Chief Procurement Officer are working together to develop a report detailing procurement integrity vulnerabilities and recommendations for reducing those vulnerabilities. In addition to this endeavor and our efforts to review major procurements on an ongoing basis, we plan to systemically assess the effectiveness of internal controls and project management at each organizational component to assure that major acquisitions are well thought out and well managed.

FINANCIAL MANAGEMENT

DHS continues to face significant financial management challenges, with some of the most critical at ICE. DHS' Chief Financial Officer is well aware of these challenges and is working to address them, although he has had limited resources to deal with these issues. DHS also faces a major challenge in implementing the *Department of Homeland Security Financial Accountability Act*, which requires that an audit of internal controls over DHS' financial reporting be performed next year.

Summary of the FY 2004 Financial Statement Audit Report

FY 2004 was the first full year of operation for the Department. Because the financial statement auditor, KPMG LLP, was able to perform more audit procedures compared to FY 2003 additional material weaknesses surfaced. Unfortunately, KPMG was unable to provide an opinion on the Department's FY 2004 statements. This disclaimer of opinion was due to circumstances at ICE, the inability to complete audit procedures over certain costs and budgetary transactions at the Coast Guard, the lack of reconciliations for intra-governmental balances, and the accelerated reporting deadline of November 15th that prevented an extension of audit procedures.

ICE presented the Department with the most critical problems. ICE's financial reporting environment underwent significant change in FY 2004. Its legacy agency, the Immigration and Naturalization Service, and the former U.S. Customs Service, were reorganized into three bureaus: ICE, Customs and Border Protection (CBP), and Citizenship and Immigration Services (CIS). ICE experienced significant budget difficulties during the year due at least in part to the late preparation of agreements to reimburse it for costs incurred on others' behalf. In FY 2004 ICE became the accounting services provider for several other Department components, as well as supporting its own and CIS' accounting needs. ICE also experienced significant staff turnover. As a result, it fell seriously behind in basic accounting functions, such as account reconciliations, analysis of material abnormal balances, and proper budgetary accounting. The auditors observed a void in the financial management infrastructure at ICE that would likely continue to jeopardize the integrity of DHS' financial reporting until the fundamental issues of internal control, including proper staffing and oversight, were addressed. We are continuing to

review the circumstances leading to these problems, and the effects they have had on ICE operations.

KPMG was unable to complete audit procedures over certain costs and budgetary transactions at the Coast Guard due to the accelerated deadlines. The Coast Guard factors significantly in many of the material weaknesses identified in the auditors' report. These material weaknesses made it much more difficult for both the Coast Guard and the auditors to complete the audit by the deadline.

The Department had significant out-of-balance conditions with other federal entities, which were not reconciled; therefore, it could not support certain balances on its own books. The most significant out-of-balance conditions existed at ICE. A lack of resources in the OCFO prevented the accountant responsible for intra-governmental reconciliations from researching and reconciling these differences in a timely manner during the year and at year-end.

The financial statement audit had to be completed three months earlier than the prior year due to the accelerated reporting deadline of November 15th. The Department had little time to focus on correcting deficiencies from KPMG's last report before it was subjected to another financial statement audit. To have a high likelihood of meeting an accelerated reporting deadline successfully, the Department's internal controls needed to be much better. The Department entered this audit with seven material weaknesses and seven other reportable conditions related to financial reporting.

Material Weaknesses and Other Reportable Conditions

KPMG identified 10 material weaknesses in internal control at DHS in FY 2004 related to:

- oversight;
- ICE;
- financial statement preparation;
- system security;
- fund balance with Treasury;
- property, plant and equipment;
- operating materials and supplies;
- accounts payable and disbursements;
- budgetary accounting; and intra-governmental; and,
- intra-departmental balances.

The auditors noted three additional reportable conditions related to deferred revenue, environmental liabilities, and custodial activity at CBP.

The most critical material weaknesses dealt with the need for additional technical resources to support the CFO in his financial reporting and oversight responsibilities, and the void in ICE's financial management infrastructure. The CFO has obtained additional resources for his office through hiring and a contractor. He has assured us that steps are underway to address the financial management issues at ICE. A new budget director at ICE was recently designated.

Additional Challenges in the Upcoming Year

The *Department of Homeland Security Financial Accountability Act* requires that an annual audit of the Department's internal control over financial reporting be performed beginning next year. Recently, OMB revised its Circular A-123, *Management's Responsibility for Internal Control*, which the Department is using to prepare for this audit. However, the success of this effort will require time given the Department's limited resources, its already significant number of material weaknesses, and the additional documentation and monitoring procedures that must be put in place.

Revenue Collection

Annually, CBP collects more that $22 billion in duties, excise taxes, fines, penalties and other revenue. CBP has had an active program to monitor trade compliance, but in the face of critical homeland security responsibilities, counter-terrorism activities have begun to claim a higher share of border resources. CBP faces a challenge in protecting trade revenue and enforcing trade laws at a time when the terrorist threat demands much more from CBP's border resources.

CBP is responsible for collecting user fees from air passengers arriving in the U.S. These fees are designed to pay for the costs of inspection services provided by CBP (which now includes the former INS and the Animal and Plant Health Inspection Service (APHIS) inspection processes). Between FYs 1998 and 2002, the former U. S. Customs Service collected $1.1 billion from the airlines. Now that CBP's inspection workforce has expanded to include the former INS and APHIS inspection services, it is important that CBP ensure that revenues collected are accounted for and are adequate to cover the costs of services provided.

CIS generates more than $2 billion in revenues through collection of application fees from non-citizens seeking entry into the U.S. In fulfilling its mission, CIS processes millions of actions and requests that are documented in paper files. The systems that track these applications are non-integrated, and many are ad hoc. Deferred revenue is a financial measure of pending applications and is material to DHS' financial statements. The challenge for CIS is to move from paper based and non-integrated processes to an integrated case management system.

GRANTS MANAGEMENT

DHS inherited a variety of grant programs, which provide money for disaster preparedness, prevention, response, and recovery. Significant shortcomings have been identified in many of these programs in the past. The potential for overlap and duplication has grown as the number of grant programs has grown. In an effort to achieve better coordination, the Office for Domestic Preparedness and Office of State and Local Coordination were consolidated into the Office of State and Local Government Coordination and Preparedness (SLGCP). That office now manages most of DHS' preparedness and first responder grant programs. The consolidation represents progress toward the one-stop shop that states and local jurisdictions have long sought.

In developing and implementing a national program to enhance the capacity of state and local agencies to respond to incidents of terrorism, DHS has integrated numerous distinct, yet related,

preparedness grant initiatives and programs into a single program under the auspices of SLGCP. Under the $2.6 billion fiscal year 2005 Homeland Security Grant Program, SLGCP consolidated the application process and administration of six programs: State Homeland Security Program, Urban Areas Security Initiative, Law Enforcement Terrorism Prevention Program, Citizen Corps, Emergency Management Performance Grants, and Metropolitan Medical Response System Program Grants.

However, much work remains to be done. In March 2004, we issued *An Audit of Distributing and Spending "First Responder" Grant Funds, OIG-04-15.* The report identified problems at the state and local level that were causing grant fund distribution and spending to be slow. The problems included too many large grant programs that had to be processed in too short a time by inadequate state and local staffing, a lack of federal guidance on preparedness standards, complex and time-consuming state and local planning processes, and burdensome state and local procurement and grant approval processes. These problems were verified by work done by GAO and the Department's Homeland Security Advisory Counsel Task Force.

The Department has taken action to implement the recommendations in our March report and to respond to GAO and task force concerns. Efforts are under way to identify and disseminate best practices, including how states and localities manage legal and procurement issues that affect grant distribution. SLGCP has established a new Homeland Security Preparedness Technical Assistance Program service to enhance the grant management capabilities of state administrative agencies. Also, DHS established a password protected web site, Lessons Learned Information Sharing, which allows states, local governments, and first responder organizations to share best practices.

In addition, SLGCP has improved grantee reporting requirements. Beginning in fiscal year 2004 and continuing in fiscal year 2005, states are required to submit Initial Strategy Implementation Plans which show how planned grant expenditures are linked to larger projects, which in turn support specific goals and objectives in the state homeland security strategy. In addition to these plans, SLGCP requires states to submit biannual strategy implementation reports showing how the actual expenditure of grant funds is linked to strategy goals and objectives.

In response to our recommendation that the Department accelerate the development of federal guidelines for first responder capabilities, equipment, training, and exercises, SLGCP is developing a standardized Weapons of Mass Destruction awareness training program and national performance standards for assessing domestic preparedness capabilities and identifying gaps in those capabilities. Homeland Security Presidential Directive-8 called for a new national preparedness goal and performance measures, standards for preparedness assessments and strategies, and a system for assessing the nation's overall preparedness. DHS issued an Interim National Preparedness Goal on April 1, 2005. This goal is a product of a capabilities-based planning process that led to the identification of core capabilities that the nation and its states, communities, and citizens need to possess. By mid-April 2005, DHS plans to issue detailed instructions on how communities can use this goal to manage federal preparedness assistance.

For FY 2006, states and urban areas are to update their Homeland Security Preparedness strategies to reflect seven national priorities in order to receive continued federal preparedness

assistance. These priorities include: 1) implement the National Incident Management System and National Response Plan; 2) expand regional collaboration; 3) implement the Interim National Infrastructure Protection Plan; 4) strengthen information sharing and collaboration capabilities; 5) strengthen interoperable communications capabilities; 6) strengthen capabilities for detection, response, and decontamination of chemical, biological, radiological, nuclear, or explosive materials; and, 7) strengthen medical surge and mass prophylaxis capabilities. For FY 2007, states and urban areas will need to revise their Homeland Security Preparedness strategies to align with the Final National Preparedness Goal in order to receive further federal preparedness assistance. DHS plans to issue the Final National Preparedness Goal and a target capabilities list, updated to include the target levels of capabilities, on October 1, 2005.

Finally, in response to our reporting that a formal grant monitoring system was lacking, DHS updated its grant-monitoring guidance in fiscal year 2004 and established new monitoring goals. According to the guidance, at least one office file review and one on-site visit should be completed for each state each fiscal year. In addition, the requirements for Initial Strategy Implementation plans and biannual strategy implementation reports, discussed earlier, should improve monitoring. As of September 2004, SLGCP filled 138 staff positions, as compared with 63 filled positions at the end of fiscal year 2003. That should help alleviate the staffing shortages, which contributed to DHS's inability to conduct frequent grantee monitoring.

Although SLGCP has program management and monitoring responsibility for its grants, it relies on the Justice Department's Office of the Comptroller for grant fund distribution and assistance with financial management support. In the department's 2004 financial statement audit report, the independent auditors noted that SLGCP management was not actively involved in the financial reporting of its activities and had not obtained a thorough understanding of the control activities over its financial reporting process performed by the Justice Department. As a result, SLGCP lacks assurance that the processing of its financial activities coincides with its business operations, are reported accurately, and controlled properly.

We are currently conducting audits of individual states' management of first responder grants, state and local governments' first responder grant spending, and analyzing the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability and needs assessments. We are also continuing our audits of FEMA's disaster relief programs as well as beginning an audit of the Urban Area Security Initiative grants.

****

Mr. Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the members may have.